Washington State DEPARTMENT OF SOCIAL & HEALTH SERVICES

DIVISION OF DEVELOPMENTAL DISABILITIES
Olympia, Washington

TITLE: COMPUTER INFORMATION SECURITY POLICY 13.03

Authority: CFR 483.410 (c)
Chapter 42.17 RCW
Chapter 70.02 RCW
Chapter 338-320 WAC
DSHS Administrative Policy 15.10

PURPOSE

The purpose of this policy is to establish policy and procedures for safeguarding and security of confidential computer-stored information, documents, and case files for Division of Developmental Disabilities (DDD) clients.

SCOPE

This policy applies to all DDD organizational units.

POLICY

Statutes and policies regarding confidentiality of written client information shall also apply to information stored electronically in computer memories, disks, tapes, and any other storage media. This shall include:

A. Client records in the Division of Developmental Disabilities Management Information Systems (DDD-MIS);

B. Any other computer files which might be drawn from the DDD-MIS; and

C. Any computer files created independently by any part of DDD, if such files contain information which is defined in statute or policy as being confidential.

DEFINITIONS

A. "Password" means a user-assigned computer system access word unique to individual users that must be used with a "user-id" to gain access to a computer-managed database of information.

B. "Security" means maintaining security of confidential, computer-stored information that includes protection from:

1. Intentional or inadvertent deletion of essential data.

2. Intentional or inadvertent alteration of data.

3. Intentional or inadvertent introduction of inaccurate data.

4. Unauthorized access to and/or copying of data.

C. "User-id" means an identification assigned by Central Office MIS user coordinator specific to one "AR" or "Administrative Responsibility" to control access to computer-stored information.

PROCEDURES

Regional administrators will develop any additional procedures necessary to implement this policy.

A. The primary responsibility for safeguarding information lies with individual computer users. Secondary responsibility lies with the MIS coordinator in each region and office/RHC. Tertiary responsibility lies with the DDD-MIS user coordinator in Central Office.

1. Terminals with access to confidential client data will not be left unattended in a state which would allow unauthorized persons to view such data.

2. Passwords will be changed by users every ninety (90) days or more often.

B. Computer users will include system documentation of security measures required for maintenance of data base integrity and confidentiality of data as part of the systems design and analysis phase. Computer users will document disaster recovery procedures and file back-up requirements.

MONITORING FUNCTION

The division's Management Information Section (MIS) shall monitor, once a year or as often as necessary, computer and data security as defined under definitions, item B., and report findings, in writing, to the Office Chief, Office of Operations Support.

SUPERSESSION

Division Policy Directive: 126
Issued September 14, 1989

Approved: /s/ Linda Johnson Date: 6/15/93
Acting Director, Division of Developmental Disabilities